SVKM's
D. J. Sanghvi College of Engineering

Program: B.Tech in Comp. Sci. and Eng.(Data Science) **Academic Year: 2022** **Duration: 3 hours**
Date: 05.01.2023
Time: 10:30 am to 01:30 pm
Subject: Information Security (Semester V) **Marks: 75**

Instructions:
(1) All Questions are Compulsory.
(2) Assume suitable data wherever required, but justify it.
(3) Answer to each new question is to be started on a fresh page.
(4) Figure to the right indicate full marks.

Question No.		**Max. Marks**
Q1 (a)	i. Describe principles of cyber security. OR ii. Explain network layer protocols used in communication, management and security.	[05] [05]
Q1 (b)	i. What is TCP IP Model? Explian all layers in detail. ii. How to prevent cyber-attacks? OR iii. What is Cyber Attack? Explain various types of cyber-attacks in brief.	[05] [05] [10]
Q2 (a)	i. Find GCD of (54,888) using Euclid's algorithm. ii. Find the remainder using Fermat's theorem, to divide 3^100,000 by 53. OR iii. Explain Transportation ciphers and encrypt following input using Simple columnar transposition techniques. Input : Geeks for Geeks Key : HACK	[05] [05] [10]
Q2 (b)	Find cipher text for given input using Hill cipher method. Consider Input : Plaintext: ACT Key: GYBNQKURP	[05]
Q3 (a)	i. How Fiestel structure of block cipher can works? **OR** ii. What are the different modes of operation in block cipher? Explain any two out of them.	[05] [05]
Q3 (b)	Explain Data Encryption Standard (DES) with an appropriate example.	[10]
Q4 (a)	i. Explain key exchange management. OR ii. In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged?	[05] [05]

Q4 (b)	In an RSA cryptosystem, a particular A uses two prime numbers, 13 and 17, to generate the public and private keys. If the public key of A is 35. Then the private key of A is …?	[10]
Q5 (a)	**Write note on any two.**	
	i. Message Digest	[05]
	ii. Sniffing	[05]
	iii. Kerberos	[05]
	iv. Phishing	[05]
Q5 (b)	Describe SHA-1 algorithm in detail?	[05]